Huddle Hub One / Huddle Hub One+

Network Security Guide

Product version 2.3 - Manual version 1

Huddle Room Technology Srl
Via Ruggero Grieco n.1/C – 41011 Campogalliano (MO)
Italy

www.hrt.website
info@hrt.email

Table of Contents

1 Introduction

1.1 Huddle Hub

Huddle Hub™ product family is the answer to the needs of modern teamwork, which is increasingly based on content presentation and video-conference. Thanks to Huddle Hub, these activities can be performed everywhere in your organization, in traditional meeting or huddle rooms, but also in offices, open-space areas, or even lounges. Every place in your company / organization - whether AV equipped or not - can be used as a huddle room:

- Taking advantage of existing large displays and webcams, but also using only individual devices. Or combining the two.
- With no cables for the TV, and no cables for the webcam.
- Running up to four concurrent sessions on a single Huddle Hub unit.
- Experiencing a smooth integration between Huddle Hub and your favorite video-conference software.

The Huddle Hub solution is made of two components:

- The Huddle Hub unit, currently available in two versions: Huddle Hub One (**HHO**) and Huddle Hub One+ (**HHO+**);
- The Huddle Hub App (**HHApp** or simply **App**), a companion software available for Windows, MacOS, iOS and Android devices. Though HHApp is the best way to unleash all the power of the Huddle Hub solution, presentations can also be received on any web browser without the need of installing any app.

The two models HHO and HHO+ are identical except for network connectivity: both models allow **wired connection**, but Huddle Hub One+ also embeds a **wireless network adapter** for Wi-Fi connectivity, thus supporting a **dual-network configuration**.

Given that HHO+ includes all the functionality of HHO, when this guide refers to HHO it means HHO or HHO+. HHO+ specific features will be highlighted with the "HHO+ only" marker.

1.2 Documentation

HRT provides a thorough and exhaustive documentation, consisting of the following manuals:

- **Quick Start Guide**: a very short guide that contains the essential steps to start using HHO and HHApp. Available in the box of the product and in the support section of HRT website (www.hrt.website).
- **Specification, Safety and Conformity**: describes all the technical specifications, the safety precautions and the conformity of HHO to national/internationals rules and certification requirements. Available in the box of the product and in the support section of HRT website (www.hrt.website).
- **User Guide**: shows the user how to use and get the most from Huddle Hub App. Available in the

support section of HRT website (www.hrt.website).

- Installation Guide: from unpacking to deployment, a short guide to install your HHO unit and choose among different network configurations. Available in the support section of HRT website (www.hrt.website).
- Configuration Guide: directed to IT Managers or IT staff members, it explains how to configure HHO to better suit the company needs. Available in the support section of HRT website (www.hrt.website).
- Network Security Guide: contains recommendations for the IT Manager or Network Security Manager, aimed at designing and implementing a secure deployment of HHO units in the organization's infrastructure. Available in the support section of HRT website (www.hrt.website).
- FAQ: the support section of HRT website (www.hrt.website) contains also a dynamically updated knowledge base with the answer to the Frequently Asked Questions.

Before consulting our documentation, please check that the product version printed on the cover page of your manual matches your HHO and HHApp versions, and that the manual version is the latest one. Manual numbering follows the following scheme:

```
<Manual name> <Product version> - <Manual version> . pdf
```

For example, "User Guide 2.0-3.pdf" means that this version of the User Guide covers all product versions staring with "2.0" (e.g. 2.0.1, 2.0.5 etc) and it's version 3 of the manual itself.

HRT supports only the latest release of its software, which is always available free of charge. Users and IT Managers are invited to keep their HHApp and HHO units up to date, and to download the most recent version the manuals from the support section of HRT website.

1.3 Purpose of this Guide

The use of HHO in unsafe network environments is perfectly legitimate: HHO units deployed in networks open to the public do not require any specific security policy.

However, when deployed in security-conscious organizations, HHO should be considered as any other network-attached device and included in the network security policy enforced by the organization. This document contains recommendations, directed to the IT or Network Security Manager, aimed at designing and implementing a secure deployment of HHO units in the organization's infrastructure.

2 Intrinsic Security

2.1 Secure Boot

HHO implements a Unified Extensible Firmware Interface (UEFI) secure boot protocol, which secures the boot process by preventing the loading of drivers or OS loaders that are not signed with HRT digital signature.

This architecture protects the unit against installation and execution of malware.

2.2 Encryption

All the video and audio streams between HHO and the connected HHApp clients are encrypted with the AES 128 algorithm.

This prevents ill-intentioned people from using a network sniffer tool to sniffs out the data flowing over your computer network between HHO and its clients (network sniffers can take snapshot copies of the data without redirecting or altering it).

3 Secure Deployment of HHO units

3.1 Connections

3.1.1 Wired Connection

To ensure maximum security, you should configure your HHO unit using a standalone network, that is a network that is not connected to your corporate network.

1. Set up a standalone network environment and make sure it has an active DHCP server.
2. Connect HHO to the standalone network by plugging its Ethernet connector.
3. Switch the unit on.
4. HHO ships with Ethernet interface and DHCP enabled, so the unit will receive an IP address. The IP address of HHO depends on your company LAN address family (e.g. 192.168.1.x), on your DHCP server and in general on your network configuration.
5. Get the IP address of the HHO unit, either attaching an HDMI display to its port (the IP address appears in the welcome screen) or using a network tool to discover which IP address it's been assigned.
6. Type the IP address in a web browser and access the Web Console of your HHO unit. Both HTTP and HTTPS connections are available; for security reasons HTTPS is the suggested mode.

3.1.2 Wireless Connection (HHO+ only)

To ensure maximum security, during this initial configuration you will configure your HHO+ unit using its dedicated Wi-Fi network, without connecting it to your corporate network.

1. Make sure your HHO+ unit Ethernet connector is not plugged to any network.
2. Switch your HHO+ unit on.
3. Open the wireless network selection screen on your computer and connect it to HHO+ network. The factory default parameters are:
   - SSID: huddlehub
   - Security: WPA2
   - Password: huddlehub
4. Once connected to the wireless network of HHO+, get its IP address, either attaching an HDMI display to its port (the IP address appears in the welcome screen) or using a network tool to discover which IP address it's been assigned. The default IP address of HHO+ on its own wireless network is 10.3.2.1, but it may have been changed by a previous configuration.
5. Type the IP address in a web browser and access the Web Console of your HHO+ unit. Both HTTP and HTTPS connections are available; for security reasons HTTPS is the suggested mode.

3.2 Secure Initial Configuration

The Huddle Hub One Configuration Guide describes how to use the Web Console to configure an HHO unit: please refer to it for the procedural details. In this guide we highlight the settings that impact on the security of your network.

Admin password (General)

The very first configuration activity you should perform is changing the default password. The password field contains the keyword to access the Web Console, and it's important to secure access to configuration options in order to avoid unauthorized changes that could compromise security.

The password can be from 5 to 48 characters long: numbers, uppercase, lowercase letters, underscore and dash are admitted; special characters and spaces are not allowed.

Choosing a secure, strong, unique password for each of your HHO units is critically important. Sharing passwords between HHO units and/or other devices or accounts is not recommended: if scammers get just one password, they can access your other devices/accounts.

The following guidelines will help you in creating a strong password:

- Make it more than 8 characters long.
- Use a combination of lower-case and upper-case characters, numbers, underscores and dashes.
- Do not choose a word or date associated with you or your organization.
- Select a combination of words with unusual capitalization, numbers, and special characters interspersed. Misspelled words are stronger because they are not in the dictionary used by attackers.
- Do not write in on paper: save it in a password-protected software vault.
- Change it periodically, or as soon as you suspect it has been discovered by unauthorized people.
- The checkbox *Show password* makes your password visible while typing and should be used with care: verify that nobody is lurking behind you, directly or through a webcam or other devices.

Passcode protection (Rooms)

When checked, a *passcode* is required to join a HHO session. The passcode is a random four digits number, automatically generated by the system when a session starts. Every new participant must type in the passcode to join the session.

Without a passcode, anyone with the HHApp installed could connect to your session and receive the presentation on his/her device screen, and unless you check the list of the connected users you may not realize that someone is lurking your content.

Passcode is checked by default and should remain checked, except in environments where security is not a concern.

Access point password (Network, HHO+ only)

We strongly recommend that you change the password field that contains the keyword for the wireless connection to HHO+. The admitted password follows the industry standard 8 to 63 characters specification. See Admin password above for tips about creating a secure, unique password.

Show password

This checkbox makes your password visible while typing and should be used with care: verify that nobody is lurking behind you, directly or through a webcam or other devices.

Hide SSID password in status

Tick this checkbox to hide your password from status page of HHO+ (recommended).

*Hide SSID password in TV welcome scree*n

Tick this checkbox to hide your password from the welcome screen in case a TV is connected (recommended, unless you want to use the onboard access point of your HHO+ unit to grant access to guests).

Share mode (Network, HHO+ only)

When the Wi-Fi network adapter of HHO+ is in Access Point mode, this parameter manages the connection between HHO+ wireless and wired interfaces and is security critical:

- *Routing + NAT*: in this case HHO manages the NAT translation, lets the Wi-Fi clients reach the company LAN resources connected, including Internet, through HHO+ Ethernet port by natting the clients addresses to the Ethernet interface. From the company LAN to HHO+ wireless network, the connection must be managed by route tables, forwarding the traffic to HHO+ Ethernet interface. There's no firewall isolation between the two subnets.
- *Routing*: the system only routes the Wi-Fi traffic to the Ethernet interface, without natting the addresses. Even in this case there's no firewall isolation between the wired and wireless subnets and the dialog between the two interfaces is managed by the company LAN route tables only.
- *Bridge*: the system creates its Wi-Fi network as an extension of the company LAN, using the same address family, for example on the same 192.160.1.0 subnet. With this configuration, the IP address of HHO+ Wi-Fi interface is the same of the wired network interface. In Bridge mode, being HHO+ Wi-Fi network an extension of the company LAN, the Wi-Fi clients are virtually on the same company LAN. For this mode, the correct Wi-Fi operation depends on HHO+ wired interface settings.
- *None*: means no connection between HHO+ Wi-Fi clients and the company LAN resources.

In the sharing modes *Routing + NAT* and *Routing*, when the *LAN access to session participants only* option is active (recommended), among all the users wirelessly connected to HHO+ access point,

only the participants of HHO+ work session can access the company LAN resources. This, however, does not enforce security of your network, because anyone running a session with the HHApp will also have access to your LAN resources.

In the sharing modes *Routing + NAT* and *Routing*, when the *Block access to private networks* option is active (recommended), clients connected to the Wi-Fi adapter will not be permitted to reach private IPv4 addresses, defined by the following ranges:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Client isolation (Network, HHO+ only)

Tick this checkbox to prevent devices wirelessly connected to HHO+ from reaching each other (recommended).

4 Deployment and Connection Scenarios

4.1 Wired Connection Only

In this configuration, your HHO unit is connected to your company LAN through its Ethernet interface, and it gets reached by the clients through your company access points. Thus, the security of the network is not affected by the presence of HHO, which rely on the access permissions you grant to your users.

Guest users access to HHO can be provided only through guest users access to the company LAN.

4.2 Wireless Connection Only - Access Point Mode (HHO+ only)

A HHO+ unit can be configured not to use the company network at all by disabling its wired interface.

With this setup, clients can only connect directly to HHO+ and present data to a physically connected TV screen, or to the screen of other connected users. The company LAN is not involved at all, the Internet cannot be reached, and all the users are actually guests.

4.3 Wireless Connection Only - Station Mode (HHO+ only)

In *Station* mode, the wireless network adapter of HHO+ is used to connect to the company LAN. This configuration is useful when the unit has to be placed in a room where a wired connection is not available.

Given that HHO+ will be reached by clients through the company LAN – and not through its own wireless network – the security consideration made in the previous Wired connection only configuration apply to this case as well.

In current version, HHO+ supports only the WPA-PSK security protocol.

4.4 Dual Network Configuration (HHO+ only)

4.4.1 Station Mode - Total Isolation

In this configuration, the wireless adapter is configured in Station Mode, and the wireless and wired network adapters of HHO+ are mutually isolated.

This configuration is useful when the company has a company network and a guest network, and the IT Manager wants to grant access to the HHO+ unit through these two networks, without giving access to the HHO+ unit itself in Access Point mode.

Accredited company users will reach HHO+ by mean of company access point and company LAN, while guest users will reach HHO+ by mean of company guest network. Access to HHO+ is entirely regulated by the company network policies.

4.4.2 Access Point Mode - Total Isolation

In this configuration, the wireless adapter is configured as Access Point, but the wireless and wired network adapters of HHO+ are mutually isolated. This is achieved by setting the wireless interface *Share mode* to *None*. HHO+ can be reached through the company network or through its onboard access point, but the two networks are not connected.

The advantage of this configuration is that guest users can be granted access rights to HHO+ through its wireless interface, by simply allowing them to connect to the onboard access point. Guest users will have no access to LAN resources or to the Internet.

Accredited company users will reach HHO+ by mean of company access point and company LAN.

Client isolation option should be checked, to protect clients wirelessly connected to that unit from being accessed by other clients wirelessly connected to the same unit.

4.4.3 Access Point Mode - Partial or No Isolation

In this configuration, the wireless adapter is configured as Access Point, and the wireless interface *Share mode* is set to *Routing+NAT*, *Routing*, or *Bridge*, there's no firewall isolation between the two networks. The HHO+ unit acts like a company LAN access point, and connection to its wireless network should follow the same security rules that the organization enforces for all the other access points.

Client isolation option should be checked, to protect connected clients from being accessed by other connected clients.

In the sharing modes *Routing + NAT* and *Routing*, when the *Block access to private networks* option is active (recommended), clients connected to the Wi-Fi adapter will not be permitted to reach private IPv4 addresses, defined by the following ranges:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

4.5 Firewall Configuration

When a HHO unit is connected to the company LAN – by mean of its wired network adapter, or of its wireless network adapter set in *Station* mode - the company firewall should allow HHO to use the following ports:

- TCP 80: Web GUI http

- TCP 443: Web GUI https*
- UDP 5353: Zeroconf Service (to reach Huddle Hub through hub_name.local)
- TCP 8443: Huddle Hub-Apps communication*
- UDP 6000: Huddle Hub discovery service
- TCP 6987, 6989, 6991, 6993, 6995, 6997: Hub Room Webviewer video streams*
- TCP 6986, 6988, 6990, 6992, 6994, 6996: Hub Room Webviewer video streams
- TCP 7209, 7219, 7229: Virtual Rooms Webviewer video streams
- TCP 7210, 7220, 7230: Virtual Rooms Webviewer video streams*
- TCP 7000-7200: Hub Room Client video streams**
- TCP 7201-7208, 7211-7218, 7221-7228: Virtual Rooms Client video streams**

* Encrypted with TLS protocol, based on self-signed TLS certificates.

** Encrypted with AES128 protocol. At the beginning of every session Huddle Hub creates a new key that is sent to the clients with a proprietary protocol through port 8443 (which is already encrypted, so the security chain is never broken).

Closing ports has the following effects:

- If you block port 80, you will not be able to the web pages through HTTP.
- If you block port 5353, you will not be able to reach the Huddle Hub unit by name (es. http://huddlehub.local) but only through its IP.
- If you block port 6000, you will not be able to reach the Huddle Hub at all.

4.6 Physical Location

The flash inside the HHO unit is cyphered, so there is no significant risk of data breach when placing the unit in an unprotected location.

To prevent thefts, however, consider an appropriate physical mounting solution that makes HHO hard to remove, like a hidden VESA mounting systems behind the display.

Index

- T -

- U -

- W -